# Logging and Monitoring Standard

## Related Policy

* 201.00 Asset and Data Protection Policy

## Purpose

The purpose of the Logging and Monitoring Standard is to build on the principles established in the Asset and Data Protection Policy and provides requirements for logging, monitoring and reporting activities for Alight systems.

## Standard Statements

### Event Capture

* 1. In reference to the data classification model where applicable and available, business critical systems, applications, and infrastructure must generate reliable logs of events that pertain to:
     1. Failed access attempts, modification, or deletion of Highly Confidential or Confidential data.
     2. Attempted change or elevation of system privilege (e.g., use of SU or sudo in UNIX, administrative IDs in Windows or Notes, etc.).
     3. Attempted violation of system security rules (e.g., firewall ACL, brute-force password hacking attempts, etc.).
     4. Access to logs.
     5. Initialization and de-activation of the logs.
     6. Activation/deactivation of network or host-based protection systems, such as anti-virus software and intrusion detection systems.
     7. Attempted change or reconfiguration of system behavior, including but not limited to:
        1. Network access control lists.
        2. Critical system configuration files (Windows registry, UNIX operating system, and Application configurations, etc.).
        3. Scheduled system tasks.
  2. Logs should contain, at minimum, the information required below:
     1. Username associated with request (where available).
     2. Identity or name of affected data, system component, or resource.
     3. IP address of user (where available) action attempted (read/write/delete, network access attempt, etc.).
     4. Success or failure indication.
     5. Resource being accessed (file, account, database row/column, URL, etc.).
     6. Timestamp (synchronized against a reliable, NTP-managed clock).
     7. Resultant action taken by system (block/allow/log/etc.).
  3. Event logging must not be deactivated or modified.
  4. Where applicable, logs for external facing technologies must be logged to a log server located on the Alight internal network.

### Review & Retention

* 1. Logs must be reviewed regularly based on the criticality table in [Appendix I](#_Appendix_I_–) for anomalies.
  2. Logs must be retained based on the criticality table in [Appendix I](#_Appendix_I_–).
  3. Internal request for log files
     1. Log files will be provided to an authorized authority by approval of the system owner.
  4. External request for log files
     1. Log files will be provided to an authorized authority by approval of the system owner, Information Risk & Security Services, and the Legal Department.
  5. Automated tools or services should be utilized to facilitate the review of logs.
  6. System owners must ensure there is an appropriate means to generate, monitor, and alert on system, network, and application events log, based on the table in [Appendix](#_Appendix_I_–).

### Protection

* 1. Audit logs and records must be protected to prevent deletion or alteration.
  2. Limit the viewing of audit logs and audit record files to only those colleagues with a business need.
  3. Access to the audit configuration settings must be restricted to privileged accounts.
  4. Logs must be stored on protected and hardened log servers wherever possible and applicable.

### Time Synchronization

* 1. All Alight systems must have their system clocks synchronized to the appropriate corporate time standard e.g., ntp.aon.com or to the appropriate timeserver for the domain.
  2. Use UTC time zone as standard, where possible.

## References and Mandates

* None

## Legal Conflicts

Alight Security Policies and Standards were drafted to address the protections found in existing laws and regulations and may be amended as necessary due to law, regulation, or business requirements. There is no intent to conflict with relevant laws or regulations. In the event of any conflict with relevant laws or regulations, they will control.

Alight Security Policies and Standards may be supplemented by other policies or standards of Alight. In the case of a conflict or ambiguity, the more specific provisions of any such policy or standard of Alight shall take precedence over the more general provisions contained in Alight Security Policies and Standards.

# Appendix I – Logging

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Review Frequency | Retention Period | Segregation Requirements | Tier Definition |
| Tier One | Daily | Retain per applicable Alight Records Retention Schedule | Required | Infrastructure that supports storing and/or processing HBI and/or MBI data defined in Data Security Classification Standard |
| Tier Two | Weekly | Retain per applicable Alight Records Retention Schedule | Recommended | Infrastructure that supports storing and/or processing LBI data defined in information Data Security Classification Standard |
| Tier Three | As needed | Retain per applicable Alight Records Retention Schedule | None | Infrastructure that supports storing and/or processing NBI data |

Alight’s Records Retention Schedules are located here: <https://newcointranet.com/Documents/Standard/U/US_Records_Retention_Schedule>

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
| Document Name | INFOSEC\_201.10 Logging and Monitoring Standard |
| Primary Contact | Alight Global Security Services | [global.security.services@aon.com](mailto:SRM.Mailbox@aon.com) |
| Version Number | 1.5 |
| Owner | Alight Global Security Services | Information Security |
| Author(s) | Alight Global Security Services | Information Security |
| Approved By | Jim Hartley, Chief Information Security Officer |
| Approval Date | May 1, 2017 |
| Effective Date | May 1, 2017 |
| Creation Date | May 2, 2011 |
| Information Classification | General Internal – Low Business Impact (Green) |

# Revision History

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Level | Date | Description | Change Summary |
| 1.0 | 2012 March | Original | Restructured due to Aon Hewitt merger |
| 1.1 | 2013 June | 2013 Annual Review | Clarified Tier definitions in the appendix |
| 1.2 | 2014 June | 2014 Annual Review | Reviewed and validated |
| 1.3 | 2015 June | 2015 Annual Review | Reviewed and validated – added Legal Conflicts, 2.4 changed SRM to Information Risk & Security Services |
| 1.4 | 2016 August | 2016 Annual Review | Clarified Tier definitions in the appendix |
| 1.5 | 2017 July | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |